

1/9/1

DIALOG(R)File 351:Derwent WPI

(c) 2001 Derwent Info Ltd. All rts. reserv.

011344737      \*\*Image available\*\*

WPI Acc No: 1997-322642/199730

XRPX Acc No: N97-267005

**Random number generator for telecommunication appts - uses speech data as**

**start value for random number generator, and field strength and time frame values as additional data**

Patent Assignee: SIEMENS AG (SIEI )

Inventor: ALBERSMANN J; EUSCHER C; MUELLER A

Number of Countries: 005    Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 781063	A2	19970625	EP 96119027	A	19961127	199730 B
DE 19548044	A1	19970626	DE 1048044	A	19951221	199731
DE 19548044	C2	19980326	DE 1048044	A	19951221	199816

Priority Applications (No Type Date): DE 1048044 A 19951221

Cited Patents: No-SR.Pub

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
-----------	------	-----	----	----------	--------------

EP 781063	A2	G	11	H04Q-007/32	
-----------	----	---	----	-------------	--

Designated States (Regional): ES FR GB IT

DE 19548044	A1	9	H04Q-007/20
-------------	----	---	-------------

DE 19548044	C2	9	H04Q-007/20
-------------	----	---	-------------

Abstract (Basic): EP 781063 A

Useful data, e.g. speech data are evaluated and a start value for

the random number generator is thus obtained. The start value is transmitted to the random number generator. Radio transmission path data, e.g. field strength values and/or system specific data (e.g. time

frame values) can be used together with speech data as the basis of the

random number generating process.

System information is evaluated as a third random number parameter

according to system values. The telephone system is a DECT/GAP specific

cordless telecommunication system.

USE/ADVANTAGE - Wireless telecommunication systems; GSM.

Generates

sufficient amount of random numbers for operation of telecommunication system.

Dwg.1/4

Title Terms: RANDOM; NUMBER; GENERATOR; TELECOMMUNICATION; APPARATUS; SPEECH; DATA; START; VALUE; RANDOM; NUMBER; GENERATOR; FIELD; STRENGTH;

TIME; FRAME; VALUE; ADD; DATA

Derwent Class: W01; W02

International Patent Class (Main): H04Q-007/20; H04Q-007/32

International Patent Class (Additional): G06F-007/58; H04B-007/26

**This Page Blank (uspto)**

File Segment: EPI

Manual Codes (EPI/S-X): W01-A05B; W01-B05A1A; W01-B05A1B; W01-B05A1C;  
W01-C01C7; W01-C02B6A; W02-C01C3; W02-C03C3B; W02-C06

?

This Page Blank (uspto)



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11) EP 0 781 063 A2

(12)

## EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:  
25.06.1997 Patentblatt 1997/26

(51) Int. Cl.<sup>6</sup>: H04Q 7/32

(21) Anmeldenummer: 96119027.9

(22) Anmeldetag: 27.11.1996

(84) Benannte Vertragsstaaten:  
ES FR GB IT

(30) Priorität: 21.12.1995 DE 19548044

(71) Anmelder: SIEMENS AKTIENGESELLSCHAFT  
80333 München (DE)

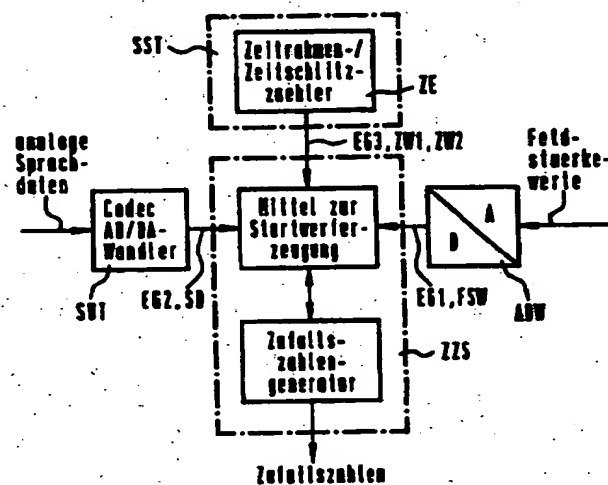
(72) Erfinder:  
• Euscher, Christoph, Dipl.-Ing.  
46414 Rhede (DE)  
• Müller, Andreas, Dipl.-Ing.  
46459 Rees (DE)  
• Albersmann, Josef, Dipl.-Ing.  
48691 Vreden (DE)

(54) Verfahren und Anordnung zum Erzeugen von Zufallszahlen in Telekommunikationsgeräten eines drahtlosen Telekommunikationssystems

(57) Um ausreichend zufällige Zufallszahlen für Telekommunikationsgeräte eines drahtlosen Telekommunikationssystems zu erzeugen, werden Nutzdaten (SD) (z.B. Sprachdaten) ausgewertet. Aus diesen Nutzdaten (SD) wird z.B. ein Startwert (STW) für die Zufallszahlenerzeugung gebildet, der einem Zufallszahlengenerator (ZZG) zugeführt wird. Als Grundlage für die

Zufallszahlenerzeugung können zusätzlich zu den Nutzdaten (SD) auch funkstreckenbezogene Daten (FSW) (z.B. Feldstärkewerte) und/oder auch systemspezifische Daten (ZW1, ZW2) (z.B. Zeitschlitz-/Zeitraumenwerte) herangezogen werden.

F 16 4



EP 0 781 063 A2

## Beschreibung

Drahtlose Telekommunikationssysteme sind Nachrichtensysteme mit einer drahtlosen Übertragungsstrecke zwischen einer Nachrichtenquelle und einer Nachrichtensenke zur Nachrichtenverarbeitung und -übertragung, bei dem an jedem x-beliebigen Ort des Nachrichtensystems (mobiler Charakter des Nachrichtensystems) die Nachrichten in einer bevorzugten Übertragungsrichtung (Simplex-Betrieb) oder in beiden Übertragungsrichtungen (Duplex-Betrieb) übertragen werden. Die Nachrichtenverarbeitung kann dabei digital oder analog sein. Darüber hinaus erfolgt die Nachrichtenverarbeitung und die drahtlose Nachrichtenübertragung vorzugsweise nach diversen Funkstandards, wie DECT (Digital European Cordless Telecommunication; vgl. (1): Nachrichtentechnik Elektronik 42 (1992, Jan./Feb.), Nr. 1, Berlin, DE; U. Pilger: "Struktur des DECT-Standards", Seiten 23 bis 29; (2): Philips Telecommunication Review, Vol. 49, Nr. 3, Sept. 1991; R. Mulder: "DECT Universal Cordless Access System", Seiten 68 bis 73;), WCPS (amerikanische DECT-Version), PAS (jap. DECT-Version), GSM einschließlich des Derivats DCS1800 (Groupe Spéciale Mobile oder Global System for Mobile Communication; vgl. Informatik Spektrum 14 (1991) Juni, Nr. 3, Berlin, DE; A. Mann: "Der GSM-Standard - Grundlage für digitale europäische Mobilfunknetze", Seiten 137 bis 152), ADC (amerikanische GSM-Version), JDC (japanische GSM-Version) etc. Als drahtlose Übertragungstechnik können neben der Funkübertragung auch andere drahtlose Übertragungsarten eingesetzt werden, wie z. B. die Infrarot-Übertragung.

"Nachricht" ist ein übergeordneter Begriff, der sowohl für den Sinngehalt (Information) als auch für die physikalische Repräsentation (Signal) steht. Signale können dabei z. B.

- (1) Bilder,
- (2) gesprochene Wörter,
- (3) geschriebene Wörter,
- (4) verschlüsselte Wörter oder Bilder

repräsentieren.

Drahtlose Telekommunikationssysteme der vorstehend umrissenen Art sind beispielsweise DECT-Systeme (Digital European Cordless Telecommunication; vgl. (1): Nachrichtentechnik Elektronik 42 (1992) Jan./Feb., Nr. 1, Berlin, DE; U. Pilger: "Struktur des DECT-Standards", Seiten 23 bis 29; (2): telcom Report 16 (1993) Nr. 1, J. H. Koch: "Digitaler Komfort für schnurlose Telekommunikation - DECT-Standard eröffnet neue Nutzungsgebiete", Seiten 26 und 27; (3): tec 2/93 - Das technische Magazin von Ascom "Wege zur universellen mobilen Telekommunikation", Seiten 35 bis 42) oder GAP-Systeme (Generic Access Profile; ETSI-Publikation prETSS00444, April 1995, Final Draft, ETSI, FR), die beispielsweise gemäß der Darstellung in FIG 1 aufgebaut sein können.

Nach dem DECT/GAP-Standard können gemäß der Darstellung in FIG 1 an einer DECT/GAP-Basisstation BS über eine für den Frequenzbereich zwischen 1,88 und 1,90 GHz ausgelegte DECT/GAP-Luftschnittstelle maximal 12 Verbindungen nach dem TDMA/FDMA/TDD-Verfahren (Time Division Multiple Access/Frequency Division Multiple Access/Time Division Duplex) parallel zu DECT/GAP-Mobilteilen MT1...MT12 aufgebaut werden. Die Zahl 12 ergibt sich aus einer Anzahl "k" von für den Duplexbetrieb eines DECT/GAP-Systems zur Verfügung stehenden Zeitschlitzten bzw. Telekommunikationskanälen (k = 12). Die Verbindung können dabei intern und/oder extern sein. Bei einer internen Verbindung können zwei an der Basisstation BS registrierte Mobilteile, z. B. das Mobilteil MT2 und das Mobilteil MT3, miteinander kommunizieren. Für den Aufbau einer externen Verbindung ist die Basisstation BS mit einem Telekommunikationsnetz TKN, z.B. in leitungsgebundener Form über eine Telekommunikationsanschlußeinheit TAE bzw. eine Nebenstellenanlage NSA mit einem leitungsgebundenen Telekommunikationsnetz oder gemäß der WO 95/05040 in drahtloser Form als Repeaterstation mit einem übergeordneten Telekommunikationsnetz, verbunden. Bei der externen Verbindung kann man mit einem Mobilteil, z. B. mit dem Mobilteil MT1, über die Basisstation BS, die Telekommunikationsanschlußeinheit TAE bzw. Nebenstellenanlage NSA mit einem Teilnehmer in dem Telekommunikationsnetz TKN kommunizieren. Besitzt die Basisstation BS - wie im Fall des Gigaset 951 (Siemens Schnurlostelefon, vgl. telcom Report 16, (1993) Heft 1, Seiten 26 und 27 - nur einen Anschluß zu der Telekommunikationsanschlußeinheit TAE bzw. der Nebenstellenanlage NSA, so kann nur eine externe Verbindung aufgebaut werden. Hat die Basisstation BS - wie im Fall des Gigaset 952 (Siemens Schnurlostelefon; vgl. telcom Report 16, (1993), Heft 1, Seiten 26 und 27) - zwei Anschlüsse zu dem Telekommunikationsnetz TKN, so ist zusätzlich zu der externen Verbindung mit dem Mobilteil MT1 eine weitere externe Verbindung von einem an die Basisstation BS angeschlossenen leitungsgebundenen Telekommunikationsendgerät TKE möglich. Dabei ist es prinzipiell auch vorstellbar, daß ein zweites Mobilteil, z. B. das Mobilteil MT12, anstelle des Telekommunikationsendgerätes TKE den zweiten Anschluß für eine externe Verbindung nutzt. Während die Mobilteile MT1...MT12 mit einer Batterie oder einem Akkumulator betrieben werden; ist die als schnurlose Klein-Vermittlungsanlage ausgebildete Basisstation BS über ein Netzanschlußgerät NAG an ein Spannungsnetz SPN angeschlossen.

FIG 2 zeigt ausgehend von der Druckschrift Components 31 (1993), Heft 6, Seiten 215 bis 218; S. Althammer, D. Brückmann: "Hochoptimierte IC's für DECT-Schnurlostelefone" den prinzipiellen Schaltungsaufbau der Basisstation BS und des Mobilteils MT. Dieser besteht aus einem Funkteil FKT, einer Signalverarbeitungseinheit SVE mit einem Signalsteuerungsteil SST

und einem Singalummformungsteil SUT, einem Taktgenerator TG, einer als Mikrocontroller  $\mu C$  ausgebildeten Zentralen Steuerung ZS, einer Schnittstelle SS und einer Stromversorgung SV, die in der dargestellten Weise miteinander verbunden sind. Die prinzipielle Funktionsweise des Schaltungsaufbaus ist beispielsweise in der vorstehend zitierten Druckschrift Components 31 (1993), Heft 6, Seiten 215 bis 218 beschrieben.

Von den genannten Schaltungseinheiten sind das Signalsteuerungsteil SST und die Schnittstelle SS für die Basisstation BS und das Mobilteil MT unterschiedlich ausgebildet. Zur Kennzeichnung dieser Unterschiede sind die das Mobilteil MT betreffende Schaltungseinheiten eingeklammert "()".

Das Signalsteuerungsteil SST ist in der Basisstation BS als Time Switch Controller TSC und in dem Mobilteil MT als Burst Mode Controller BMC ausgebildet. Der wesentliche Unterschied zwischen den beiden Signalsteuerungsteilen TSC, BMC besteht darin, daß der basisstationsspezifische Signalsteuerungsteil TSC gegenüber dem mobilteilspezifischen Signalsteuerungsteil BMC zusätzlich Vermittlungsfunktionen (Switch-Funktionen) übernimmt.

Die Schnittstelle SS ist in der Basisstation BS als Leitungs-/BOF-Schnittstelle LBSS und in dem Mobilteil MT als BOF-Schnittstelle ausgebildet. Über die Leitungs-/BOF-Schnittstelle LBSS ist

- a) die Basisstation BS an das, z.B. leitungsgebundene, Telekommunikationsnetz TKN angeschlossen und
- b) eine gegebenenfalls vorhandene basisstationsspezifische Bedienoberfläche BS-BOF mit den übrigen Schaltungseinheiten der Basisstation BS verbunden.

Über die BOF-Schnittstelle BSS ist eine mobilteilspezifische Bedienoberfläche MT-BOF mit den übrigen Schaltungseinheiten des Mobilteils MT verbunden. Die basisstationsspezifische Bedienoberfläche BS-BOF und die mobilteilspezifische Bedienoberfläche MT-BOF weisen jeweils eine Tastatur TA, eine Anzeigeeinrichtung (Display) AE, ein Mikrofon MF, eine Hörkapsel HK und eine Tonruftklingel TRK auf.

In dem DECT-System nach FIG 1 müssen die systemimmanenten DECT-Geräte, das Schnurlos-Mobilteil MT und die Schnurlos-Basisstation BS, im Rahmen des DECT/GAP-Standards ein Paket von Standardprozeduren durchführen können. Zu diesem Paket gehören die basisstationsspezifischen Standardprozeduren "Authentifizierung des Mobilteils MT (Portable Termination PT)" und "Authentifizierung der Basisstation BS (Fixed Termination FT)" sowie die mobilteilspezifischen bzw. basisstations- und mobilteilspezifischen Standardprozeduren "Authentifizierung des Benutzers" und "Tastenzuweisung" (engl. Key Allocation). Diese in dem DECT-Standard (vgl. ETSI-Publikation ETS 300 175-5, Kap. 13.3, Okt. 1992 u. ETS 300 175-7, Kap. 4-6, insb. Kap. 4 IVm Figur 1, den Abschnitt

"Vorwort" und den Abschnitt "Einführung", Okt. 1992) als Mobility Management-Prozeduren bezeichneten Standardprozeduren sind Bestandteil des Sicherheitskonzeptes im GAP-Standard, ETSI-Publikation prETS 300 444, Kap. 8.23-8.25 und 8.32-8.34, April 1995, bei dem sich die Basisstation und das Mobilteil gegenseitig authentisieren. Darüber hinaus stehen die genannten Standardprozeduren in enger Beziehung zur Verschlüsselungseinheit im DECT-Standard (engl. encryption unit). Um die genannten Standardprozeduren ausführen zu können, muß das DECT/GAP-Gerät in der Lage sein, eine Zufallszahl mit "n" Bits zu erzeugen.

Hierfür werden beispielsweise in den DECT-Geräten Generatoren für Pseudozufallszahlen benutzt, die z.B. durch die in dem Gerät implementierte Software realisiert werden. Diese Zufallszahlengeneratoren generieren nur dann zufällige Zahlen, wenn sie einen zufälligen Startwert (im DECT-Standard wird dieser Startwert mit "seed" bezeichnet) haben. Wird in den Zufallszahlengeneratoren immer der gleiche Startwert verwendet, so erhält man auch jeweils immer die gleiche Zufallszahlenfolge.

Bisher ist es üblich gewesen, daß beim Einschalten des DECT-Gerätes ein Zähler gestartet wird, der nach einer bestimmten Zeit immer wieder inkrementiert wird. Neben dem zusätzlichen Aufwand für Zählerinkrementierung hat die Methode den Nachteil, daß zu gleichen Zeitpunkten nach dem Einschalten immer die gleichen Zufallszahlen erzeugt werden. Dies ist besonders problematisch bei der direkt nach dem Einschalten des DECT-Gerätes durchgeführten basisstationsspezifischen Standardprozedur "Authentifizierung des Mobilteils MT", weil beispielsweise der Fall eintreten kann, daß zum Zeitpunkt der Erzeugung der Zufallszahlen jeweils die gleiche Zeitspanne seit dem Einschalten vergangen ist und daher die gleichen Zufallszahlen erzeugt werden.

Außerdem ist es bisher üblich gewesen, daß der Startwert aus dem Inhalt eines Registers in dem Mikrocontroller ermittelt wird. Da aber in diesen Registern des Mikrocontrollers auch Funktionsübergabeparameter und andere deterministische Werte stehen, sind diese Inhalte nicht ausreichend zufällig.

Weiterhin ist es aus dem GSM-Standard (Groupe Spéciale Mobile oder Global System for Mobile Communication; vgl. Informatik Spektrum 14 (1991) Juni, Nr. 3, Berlin, DE; A.Mann: "Der GSM-Standard - Grundlage für digitale europäische Mobilfunknetze", Seiten 137 bis 152) und nach diesem Standard entwickelten Mobilfunkgeräten bekannt, sowohl Zeitschlitz-/Zeitrahmeninformationen als auch in den Funknachrichten enthaltene funkstreckenbezogene Informationen für die Erzeugung von Zufallszahlen heranzuziehen.

Die der Erfindung zugrundeliegende Aufgabe besteht darin, ausreichend zufällige Zufallszahlen für Telekommunikationsgeräte eines drahtlosen Telekommunikationssystems zu erzeugen.

Diese Aufgabe wird durch die Merkmale des Patentanspruches 1 und durch die Merkmale des

Patentanspruches 11 gelöst.

Die der Erfindung zugrundeliegende Idee besteht darin, daß - um ausreichend zufällige Zufallszahlen für Telekommunikationsgeräte eines drahtlosen Telekommunikationssystems zu erzeugen - Nutzdaten (z.B. Sprachdaten gemäß Ansprüche 2 und 11) ausgewertet werden.

Aus diesen Nutzdaten wird z.B. ein Startwert (Ansprüche 8 und 18) für die Zufallszahlenerzeugung gebildet, der einem Zufallszahlengenerator zugeführt wird.

Als Grundlage für die Zufallszahlenerzeugung können zusätzlich zu den Nutzdaten auch funkstreckenbezogene Daten gemäß den Ansprüchen 3, 4, 13 und 14 (z.B. Feldstärkewerte gemäß den Ansprüchen 5 und 15) und/oder auch systemspezifische Daten gemäß den Ansprüchen 3, 6, 13 und 16 (z.B. Zeitschlitz-/Zeitrahmenwerte gemäß den Ansprüchen 7 und 17) herangezogen werden.

Weitere vorteilhafte Weiterbildungen der Erfindung sind in den übrigen Unteransprüchen angegeben.

Ein Ausführungsbeispiel der Erfindung wird anhand der Figuren 3 und 4 erläutert. Es zeigen:

FIG 3 den prinzipiellen Aufbau eines Schnurlostelefons, Schnurlos-Basisstation und Schnurlos-Mobilteil, mit einem Zufallszahlengenerator

FIG 4 den prinzipiellen Aufbau des Zufallszahlengenerators nach FIG 3

FIG 3 zeigt ausgehend von dem Schaltungsaufbau der Schnurlos-Basisstation BS und dem Schnurlos-Mobilteil MT nach FIG 2 den modifizierten erweiterten Schaltungsaufbau einer Schnurlos-Basisstation BS<sub>me</sub> und einem Schnurlos-Mobilteil MT<sub>me</sub>. Die Schnurlos-Basisstation BS<sub>me</sub> und das Schnurlos-Mobilteil MT<sub>me</sub> weisen gegenüber der bekannten Basisstation BS und dem bekannten Mobilteil MT nach FIG 2 eine Zufallszahlensteuerung ZZS auf, die in der Zentralen Steuerung ZS integriert und implementiert ist. In dieser Zufallszahlensteuerung ZZS werden Zufallszahlen für die Durchführung der in der Beschreibungseinleitung erwähnten Standardprozeduren erzeugt. Die Erzeugung dieser Zufallszahlen erfolgt aufgrund von drei Eingangsgrößen, einer funkstreckenbehafteten ersten Eingangsgröße EG1, einer funkmachrichtenbehafteten zweiten Eingangsgröße EG2 und einer systemspezifischen dritten Eingangsgröße EG3.

Die erste Eingangsgröße EG1 enthält digitale Feldstärkewerte FSW (Radio Signal Strength Values RSSV), die als analoge Signale in einer dem Funkteil FKT zugeordneten Feldstärkemeßeinrichtung FSME (Radio Signal Strength Indicator RSSI) gemessen und in einem Analog/Digitalwandler ADW durch Umwandlung der analogen Signale erzeugt werden.

Die zweite Eingangsgröße EG2 enthält digitale Sprachdaten SD, die als analoge Sprachdaten von der Schnittstelle SS und dem Funkteil FKT erfaßt und in der

Signalverarbeitungseinheit SVE von dem Signalsteuerteil SST und dem Signalumformungsteil SUT aus den analogen Sprachdaten erzeugt werden.

Die dritte Eingangsgröße EG3 enthält einen ersten Zählerwert ZW1 und/oder einen zweiten Zählerwert ZW2, der/die in einer Zähleinrichtung ZE mit einem Zeitschlitzzähler und/oder einem Zeitrahmenzähler des Signalsteuerungsteils SST erzeugt werden. Die von der Zähleinrichtung ZE erzeugten Zählerwerte ZW1, ZW2 lassen sich bei dem vorliegenden DECT-spezifischen Schnurlostelefon BS<sub>me</sub>, MT<sub>me</sub> aus der DECT-spezifischen TDMA-Rahmenstruktur ableiten. Dabei wird selbst bei gleichen Zeitpunkten nach dem Einschalten ein unterschiedlicher Wert erzeugt, weil der Zeitschlitzzähler entsprechend der Kanalbelegung variieren wird.

FIG 4 zeigt den Aufbau der Zufallszahlensteuerung ZZS. Die Zufallszahlensteuerung ZZS weist danach Mittel zur Startwerterzeugung MSE und einen Zufallszahlengenerator ZZG auf. Die Mittel zur Startwerterzeugung MSE bilden aus den Eingangsgrößen EG1...EG3 nach FIG 3 einen Startwert STW zur Erzeugung von Zufallszahlen, der dem Zufallszahlengenerator zugeführt wird. Der Zufallszahlengenerator ZZG erzeugt aus dem Startwert STW schließlich die für die Durchführung der in der Beschreibungseinleitung erläuterten Standardprozeduren benötigten Zufallszahlen.

#### Patentansprüche

1. Verfahren zum Erzeugen von Zufallszahlen in Telekommunikationsgeräten eines drahtlosen Telekommunikationssystems mit folgendem Verfahrensmerkmal:  
eine von dem Telekommunikationsgerät empfangene/gesendete Nutznachricht wird als ein erster Zufallszahlenparameter (EG2) in bezug auf Nutzdaten (SD) derart ausgewertet, daß mit den Nutzdaten (SD) die Zufallszahlen erzeugbar sind.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Nutznachricht eine Sprachnachricht ist und die Nutzdaten (SD) Sprachdaten sind.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß zusätzlich zu dem ersten Zufallszahlenparameter (EG2) mindestens ein weiterer Zufallszahlenparameter (EG1, EG3) in bezug auf dem weiteren Zufallszahlenparameter immanente Daten (FSW, ZW1, ZW2) ausgewertet wird und daß die Zufallszahlen aus den Nutzdaten (SD) und den weiteren Daten (FSW, ZW1, ZW2) erzeugt werden.
4. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß eine von dem Telekommunikationsgerät empfangene Funkstreckeninformation als ein zweiter Zufallszahlenparameter (EG1) in bezug auf Funkstreckenwerte (FSW) ausgewertet wird.



5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Funkstreckeninformation eine Feldstärkeinformation ist und die Funkstreckenwerte (FSW) Feldstärkewerte sind.

6. Verfahren nach Anspruch 3, 4 oder 5, dadurch gekennzeichnet, daß eine Systeminformation als ein dritter Zufallszahlenparameter (EG3) in bezug auf Systemwerte (ZW1, ZW2) ausgewertet wird.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß die Systeminformation eine Zeitschlitz-/Zeitraheninformation ist und die Systemwerte (ZW1, ZW2) Zeitschlitz-/Zeitrahenwerte sind.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß ein Startwert (STW) zum Erzeugen der Zufallszahlen aus den Nutzdaten (SD), den Funkstreckenwerten (FSW) und/oder den Systemwerten (ZW1, ZW2) ermittelt wird.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß ein DECT-/GAP-spezifisches, mindestens aus einer Zelle bestehendes Schnurlos-Telekommunikationssystem als drahtloses Telekommunikationssystem und ein DECT-/GAP-spezifisches Schnurlos-Mobilteil (MT<sub>me</sub>) als Telekommunikationsgerät verwendet werden.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß ein DECT-/GAP-spezifisches, mindestens aus einer Zelle bestehendes Schnurlos-Telekommunikationssystem als drahtloses Telekommunikationssystem und eine DECT-/GAP-spezifische Schnurlos-Basisstation (BS<sub>me</sub>) als Telekommunikationsgerät verwendet werden.

11. Anordnung zum Erzeugen von Zufallszahlen in Telekommunikationsgeräten eines drahtlosen Telekommunikationssystems, mit folgenden Anordnungsmerkmalen:

(a) erste Erfassungsmittel (SS, FKT), die derart ausgebildet sind, daß eine von dem Telekommunikationsgerät empfangene/gesendete Nutznachricht als ein erster Zufallszahlenparameter (EG2) erfaßt wird

(b) Auswertemittel (SUT, SST), die mit den ersten Erfassungsmitteln (SS, FKT) verbunden und derart ausgebildet sind, daß die empfangene/gesendete Nutznachricht in bezug auf Nutzdaten (SD) ausgewertet wird,

(c) Erzeugungsmittel (ZZS, MFE, ZZG), die mit den Auswertemitteln (SUT, SST) verbunden und derart ausgebildet sind, daß mit den Nutzdaten (SD) die Zufallszahlen erzeugbar sind.

12. Anordnung nach Anspruch 11, dadurch gekennzeichnet, daß die die Nutznachricht eine Sprachnachricht ist und die Nutzdaten (SD) Sprachdaten sind.

13. Anordnung nach Anspruch 11 oder 12, dadurch gekennzeichnet, daß

(a) weitere Erfassungsmittel (FKT) vorgesehen sind, die derart ausgebildet sind, daß zusätzlich zu dem ersten Zufallszahlenparameter (EG2) mindestens ein weiterer Zufallszahlenparameter (EG1, EG3) erfaßt wird,

weitere Auswertemittel (FSME, ADW, ZE) vorgesehen sind, die derart ausgebildet sind, daß der/die weitere/n Zufallszahlenparameter (EG1, EG3) in bezug auf dem/den weiteren Zufallszahlenparameter immanente Daten (FSW, ZW1, ZW2) ausgewertet wird/werden.

14. Anordnung nach Anspruch 13, dadurch gekennzeichnet, daß

(a) zweite Erfassungsmittel (FKT) vorgesehen sind, die derart ausgebildet sind, daß eine von dem Telekommunikationsgerät empfangene Funkstreckeninformation als ein zweiter Zufallszahlenparameter (EG1) erfaßt wird,

(b) zweite Auswertemittel (FSME, ADW) vorgesehen sind, die derart ausgebildet sind, daß die Funkstreckeninformation in bezug auf Funkstreckenwerte (FSW) ausgewertet wird.

15. Anordnung nach Anspruch 14, dadurch gekennzeichnet, daß die Funkstreckeninformation eine Feldstärkeinformation ist und die Funkstreckenwerte (FSW) Feldstärkewerte sind.

16. Anordnung nach Anspruch 13, 14 oder 15, dadurch gekennzeichnet, daß

(a) dritte Erfassungsmittel (FKT) vorgesehen sind, die derart ausgebildet sind, daß eine von dem Telekommunikationsgerät empfangene Systeminformation als ein dritter Zufallszahlenparameter (EG3) erfaßt wird,

(b) dritte Auswertemittel (ZE) vorgesehen sind, die derart ausgebildet sind, daß die Systeminformation in bezug auf Systemwerte (ZW1, ZW2) ausgewertet wird.

17. Anordnung nach Anspruch 16, dadurch gekennzeichnet, daß die Systeminformation eine Zeitschlitz-/Zeitraheninformation ist und die Systemwerte (ZW1, ZW2) Zeitschlitz-/Zeitrahenwerte sind.

18. Anordnung nach einem der Ansprüche 11 bis 17,

dadurch gekennzeichnet, daß die Erzeugungsmittel (ZZS, MFE, ZZG) derart ausgebildet sind, daß aus den Nutzdaten (SD), den Funkstreckenwerten (FSW) und/oder den Systemwerten (ZW1, ZW2) ein Startwert (STW) zum Erzeugen der Zufallszahlen ermittelt wird. 5

19. Anordnung nach einem der Ansprüche 11 bis 18, dadurch gekennzeichnet, daß das drahtlose Telekommunikationssystem als ein DECT-spezifisches/GAP-spezifisches, mindestens aus einer Zelle bestehendes Schnurlos-Telekommunikationssystem und das Telekommunikationsgerät als ein DECT-/GAP-spezifisches Schnurlos-Mobitell (MT<sub>me</sub>) ausgebildet sind. 10 15

20. Anordnung nach einem der Ansprüche 11 bis 19, dadurch gekennzeichnet, daß das drahtlose Telekommunikationssystem als ein DECT-spezifisches/GAP-spezifisches, mindestens aus einer Zelle bestehendes Schnurlos-Telekommunikationssystem und das Telekommunikationsgerät als eine DECT-/GAP-spezifische Schnurlos-Basisstation (BS<sub>me</sub>) als Telekommunikationsgerät ausgebildet sind. 20 25

30

35

40

45

50

55

FIG 1

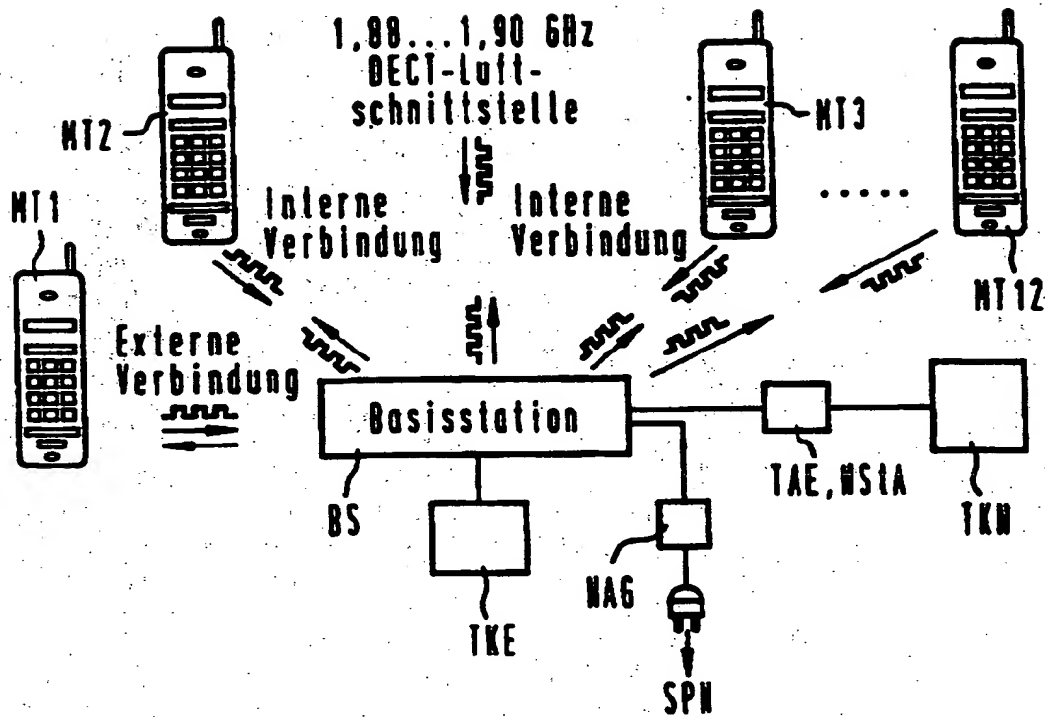
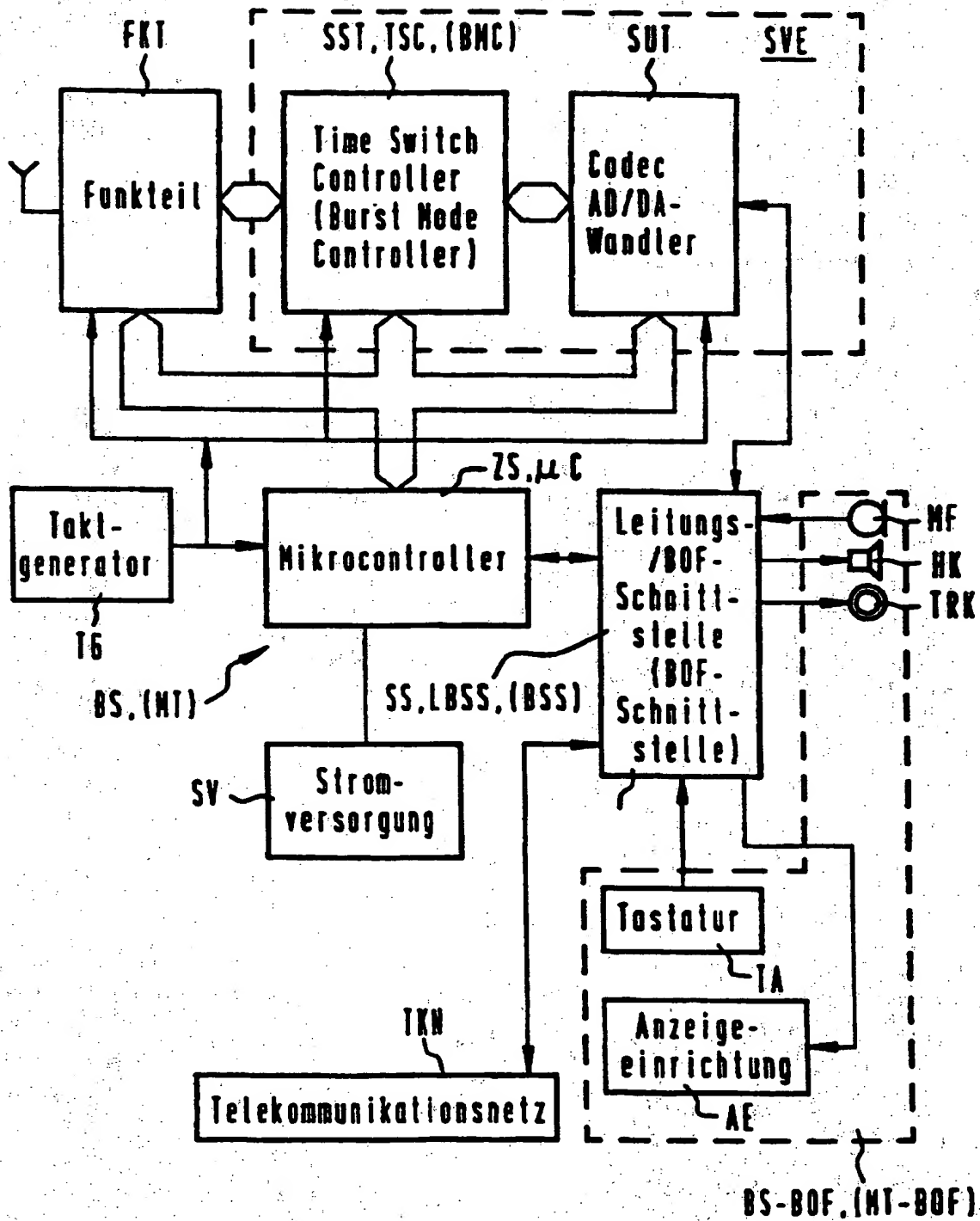


FIG 2



F163

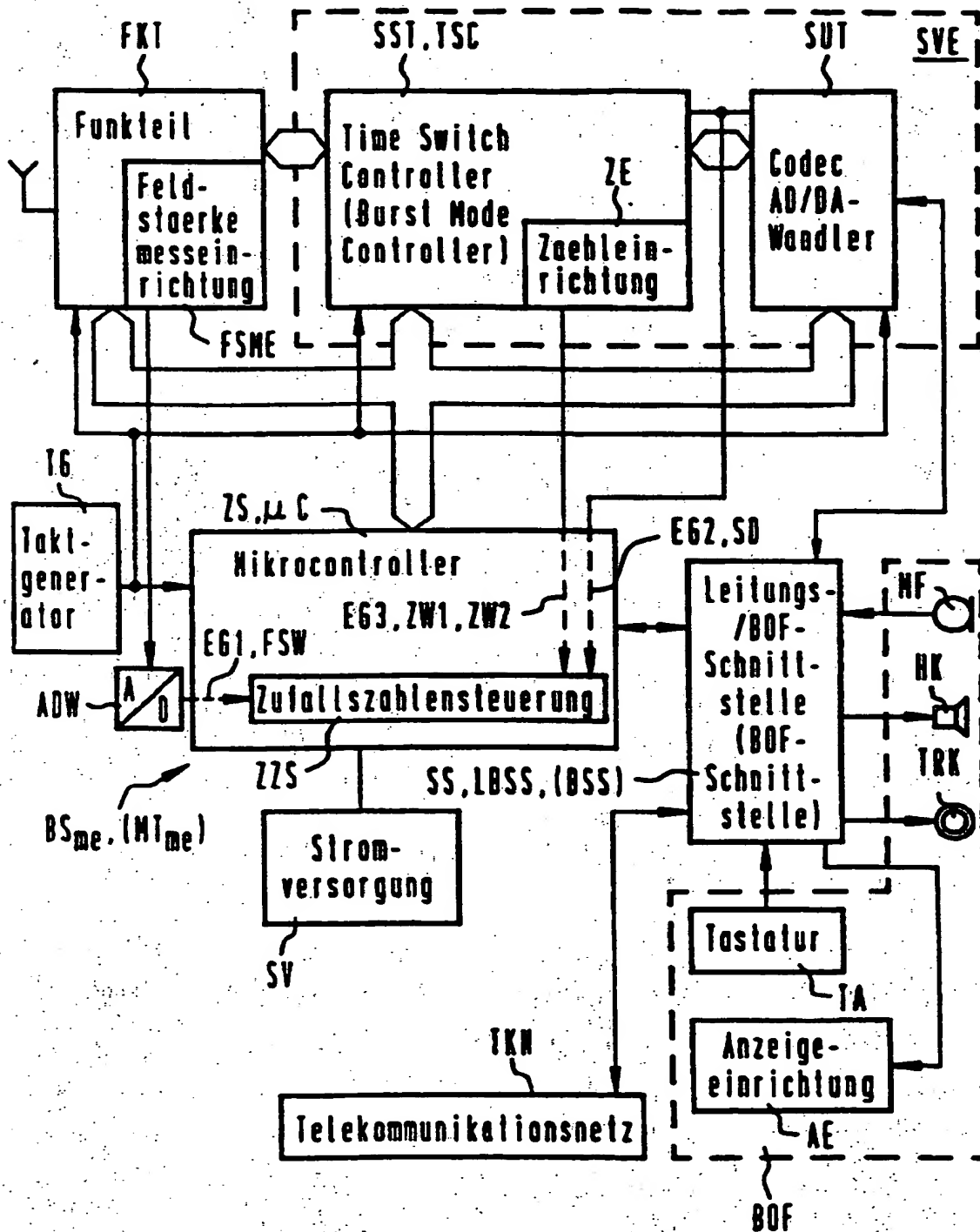


FIG 4

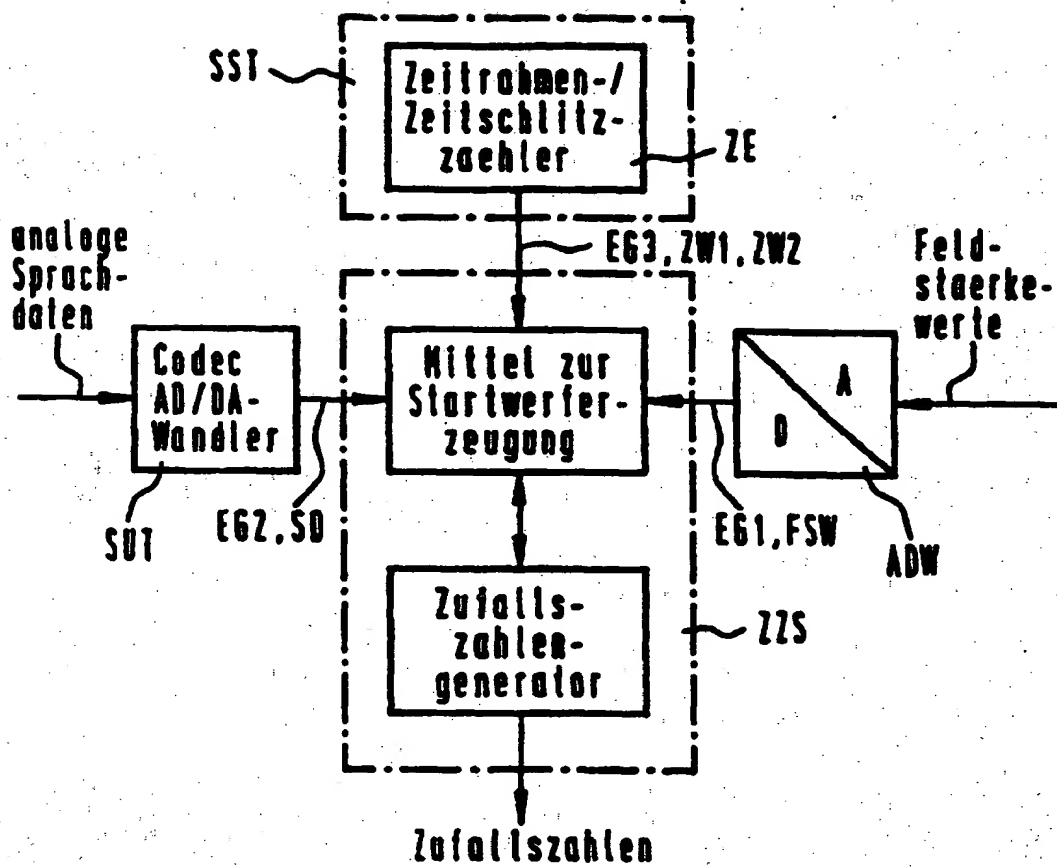


FIG 1

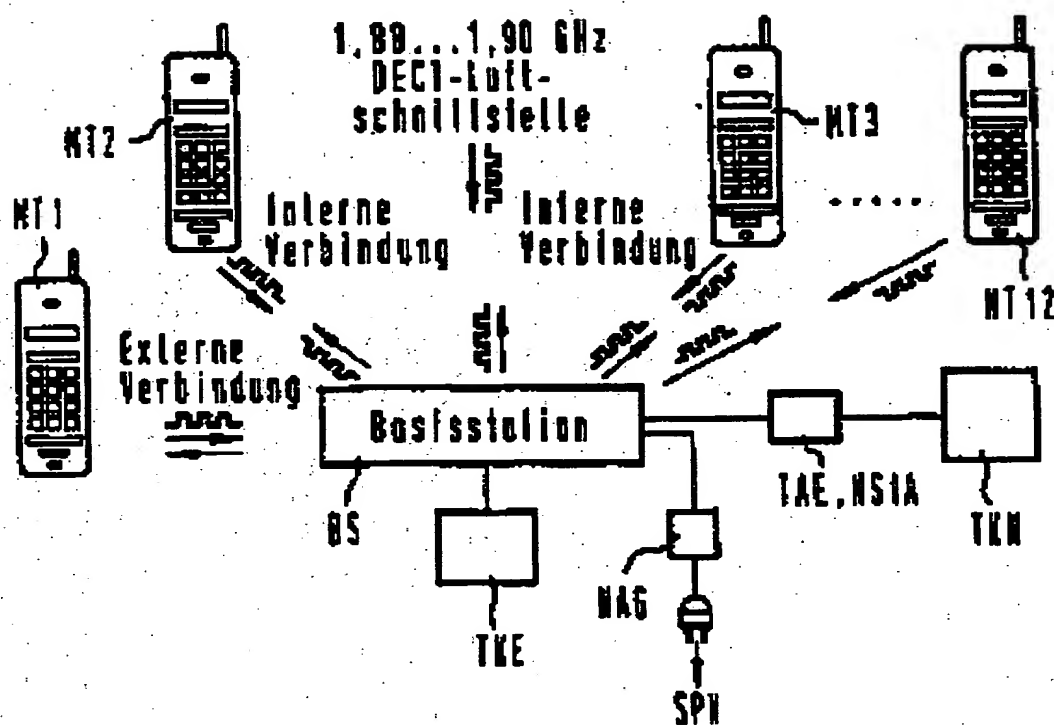
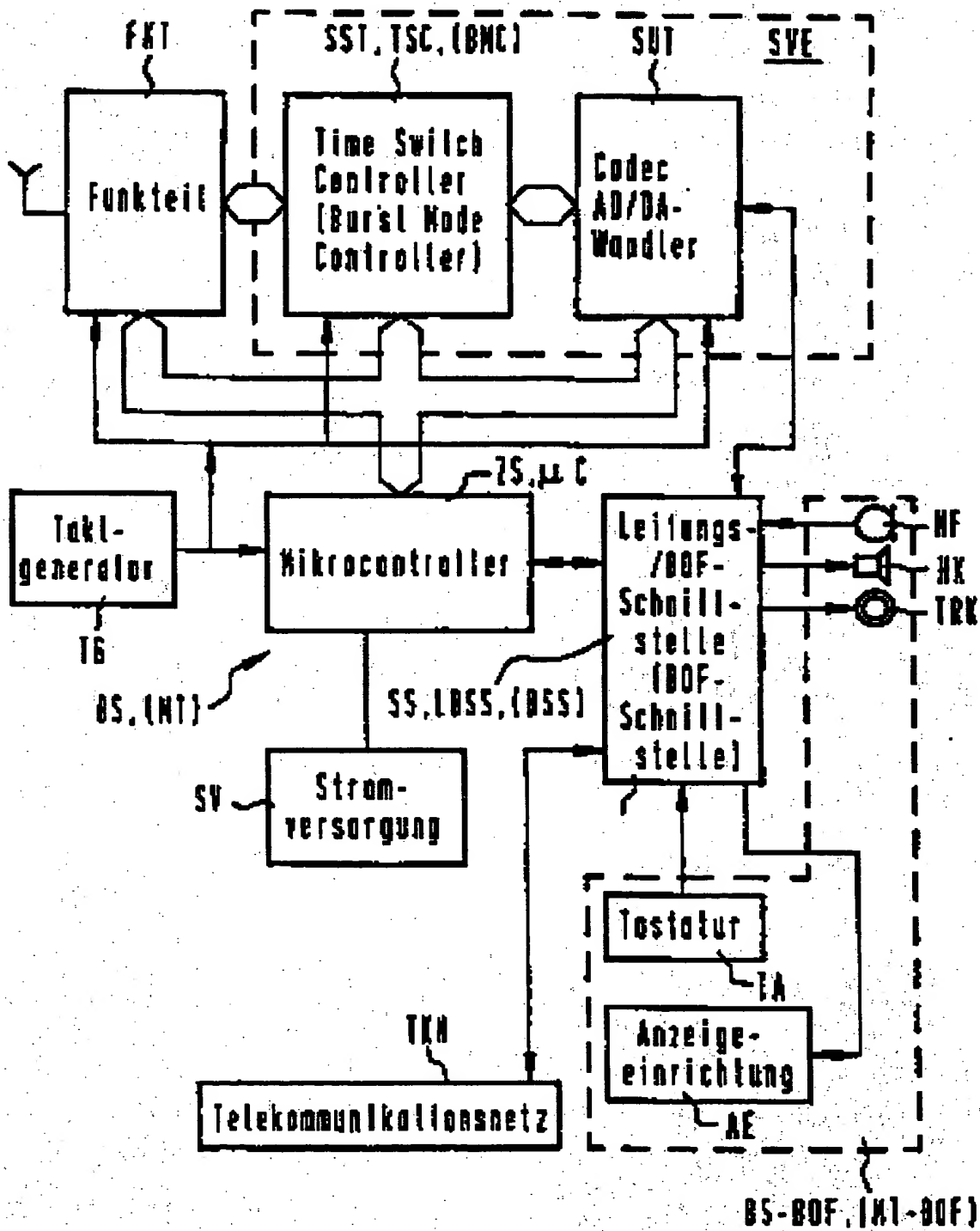


FIG 2





F163

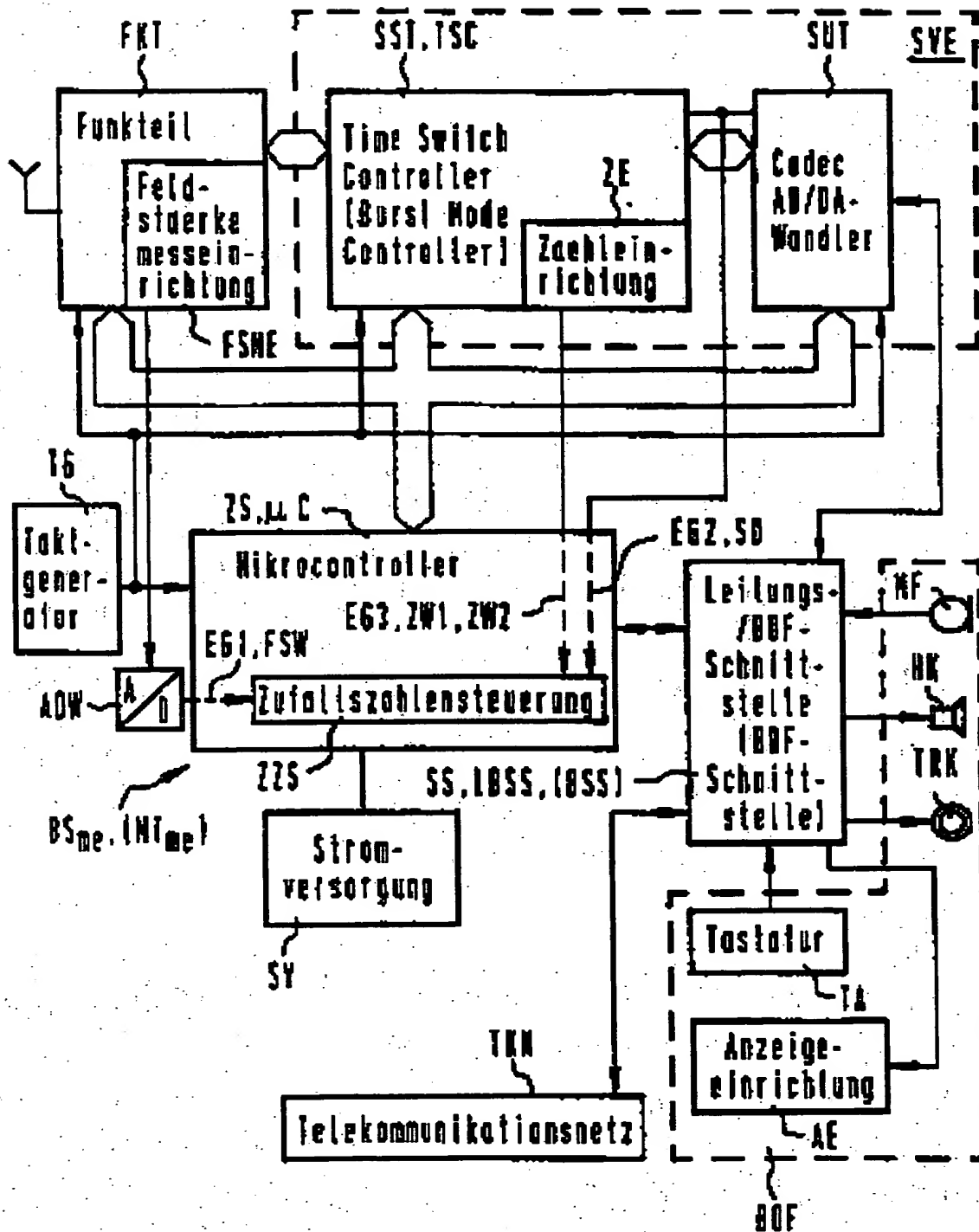
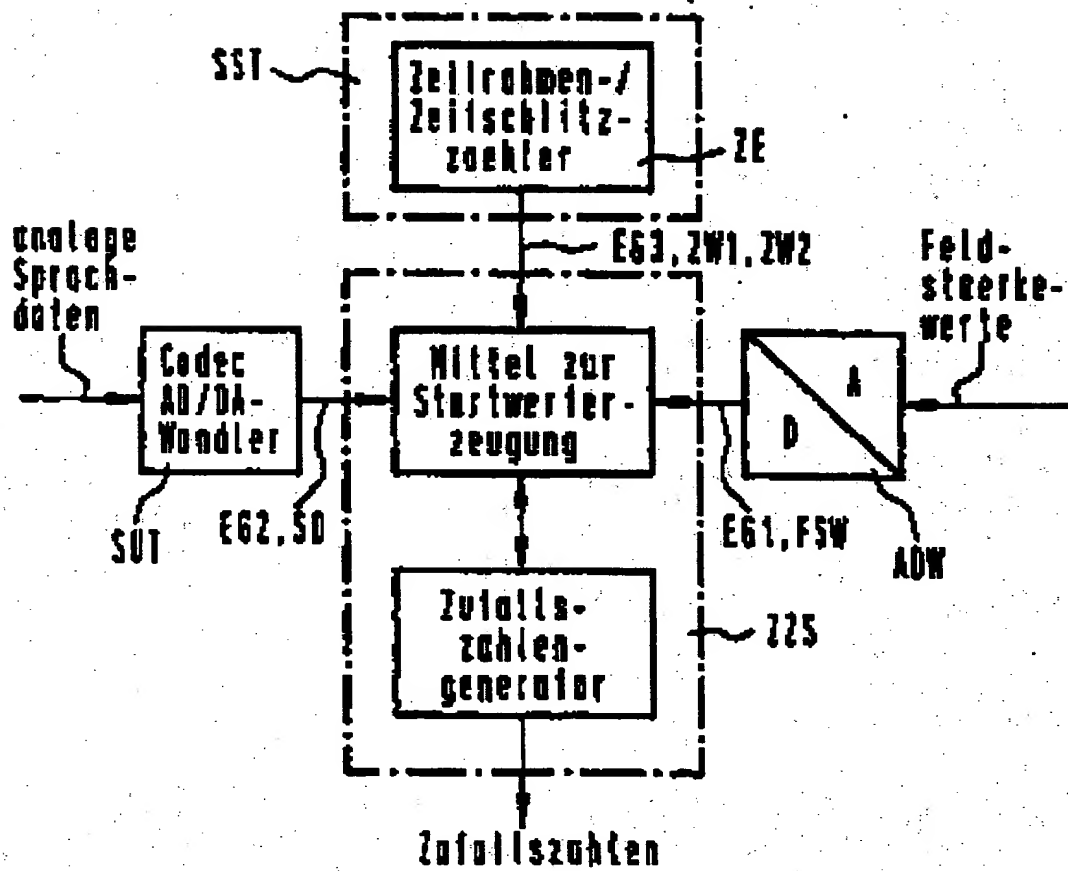


FIG 4



(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 781 063 A3

(12)

## EUROPÄISCHE PATENTANMELDUNG

(88) Veröffentlichungstag A3:  
11.08.1999 Patentblatt 1999/32

(51) Int. Cl.<sup>6</sup>: H04Q 7/32

(43) Veröffentlichungstag A2:  
25.06.1997 Patentblatt 1997/26

(21) Anmeldenummer: 96119027.9

(22) Anmeldetag: 27.11.1996

(84) Benannte Vertragsstaaten:  
ES FR GB IT

(30) Priorität: 21.12.1995 DE 19548044

(71) Anmelder:  
SIEMENS AKTIENGESELLSCHAFT  
80333 München (DE)

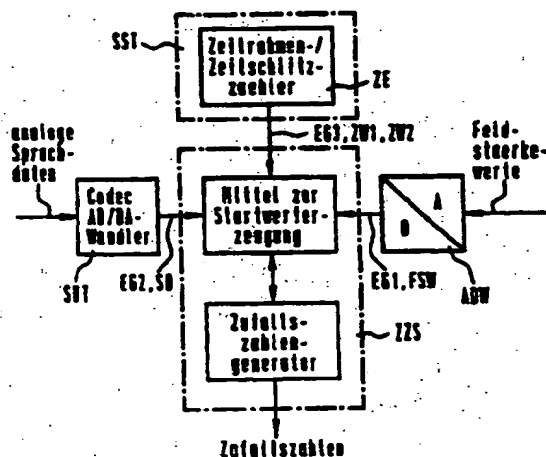
(72) Erfinder:

- Euscher, Christoph, Dipl.-Ing.  
46414 Rhede (DE)
- Müller, Andreas, Dipl.-Ing.  
46459 Rees (DE)
- Albersmann, Josef, Dipl.-Ing.  
48691 Vreden (DE)

(54) Verfahren und Anordnung zum Erzeugen von Zufallszahlen in Telekommunikationsgeräten eines drahtlosen Telekommunikationssystems

(57) Um ausreichend zufällige Zufallszahlen für Telekommunikationsgeräte eines drahtlosen Telekommunikationssystems zu erzeugen, werden Nutzdaten (SD) (z.B. Sprachdaten) ausgewertet. Aus diesen Nutzdaten (SD) wird z.B. ein Startwert (STW) für die Zufallszahlenerzeugung gebildet, der einem Zufallszahlengenerator (ZZG) zugeführt wird. Als Grundlage für die Zufallszahlenerzeugung können zusätzlich zu den Nutzdaten (SD) auch funkstreckenbezogene Daten (FSW) (z.B. Feldstärkewerte) und/oder auch systemspezifische Daten (ZW1, ZW2) (z.B. Zeitschlitz-/Zeitraumenwerte) herangezogen werden.

FIG 4



EP 0 781 063 A3



Europäisches  
Patentamt

# EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung  
EP 96 11 9027

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.C1.6)
X	WO 91 01067 A (MOTOROLA INC) 24. Januar 1991 * Seite 8, Zeile 5 - Zeile 27 *	1, 3, 6, 11, 13	H04Q7/32
A	WO 92 02089 A (ERICSSON GE MOBILE COMMUNICAT) 6. Februar 1992 * Seite 21, Zeile 20 - Zeile 25; Abbildung 5 *	1, 11	
			RECHERCHIERTE SACHGEBIETE (Int.C1.6)
			H04Q G06F H03K H04L H04K
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort BERLIN		Abschlußdatum der Recherche 18. Juni 1999	Prüfer Leouffre, M
<p><b>KATEGORIE DER GENANNTEN DOKUMENTE</b></p> <p>X : von besonderer Bedeutung allein betrachtet  Y : von besonderer Bedeutung in Verbindung mit einer  anderen Veröffentlichung derselben Kategorie  A : technologischer Hintergrund  O : nichtschriftliche Offenbarung  P : Zwischenliteratur</p> <p>T : der Erfindung zugrunde liegende Theorien oder Grundsätze  E : älteres Patentedokument, das jedoch erst am oder  nach dem Anmeldedatum veröffentlicht worden ist  D : in der Anmeldung angeführtes Dokument  L : aus anderen Gründen angeführtes Dokument  &amp; : Mitglied der gleichen Patentfamilie, übereinstimmendes  Dokument</p>			

**ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT  
 ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.**

EP 96 11 9027

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentedokumente angegeben.  
 Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am  
 Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

18-06-1999

Im Recherchenbericht angeführtes Patentedokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9101067 A	24-01-1991	AU 6034790 A	06-02-1991
		CA 2063447 A,C	13-01-1991
		IL 94467 A	31-12-1995
		JP 2684118 B	03-12-1997
		JP 5503816 T	17-06-1993
		MX 166091 B	17-12-1992
		US 5239294 A	24-08-1993
WO 9202089 A	06-02-1992	AU 645464 B	13-01-1994
		AU 8433191 A	18-02-1992
		CA 2087616 A	21-01-1992
		CN 1059999 A,B	01-04-1992
		GB 2261348 A,B	12-05-1993
		HK 29795 A	10-03-1995
		JP 2688659 B	10-12-1997
		JP 6501350 T	10-02-1994
		KR 9608031 B	19-06-1996
		NZ 238651 A	27-04-1994
		NZ 248445 A	25-03-1994
		SG 178094 G	12-05-1995
		US 5148485 A	15-09-1992

EPO FORM P0481

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts. Nr.12/82

This Page Blank (uspto)